UNITED STATES DISTRICT COURT FOR THE MIDDLE DISTRICT OF TENNESSEE

JEFFREY SKLAR, DC, individually and on behalf of all others similarly situated, Plaintiff, v. CHANGE HEALTHCARE INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jeffrey Sklar, DC ("Plaintiff"), by and through the undersigned counsel, brings this class action complaint against Defendant Change Healthcare Inc. ("Defendant" or "Change"), on behalf of himself and all others similarly situated. Plaintiff makes the following allegations based upon personal knowledge as to his own actions and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. Plaintiff's and Class Members' business operations have been harmed by the Defendant's failure to secure and safeguard their information systems from a foreseeable cyberattack.

2. Change is a healthcare technology company that connects providers, payers, patients, and pharmacies. The services are central to the U.S. healthcare system. It is a subsidiary of UnitedHealth Group ("UHG").

3. On February 21, 2024, Change disclosed that it was the subject of a massive data breach (the "Data Breach"). A ransomware group, "ALPHV/Blackcat" ("Blackcat"), claims to

have gained unauthorized access to Change's networks. Change suffered network outages when Blackcat seized 6 terabytes of critical confidential and highly sensitive information and encrypted portions of Change's networks. Millions of patients and physicians have been impacted by the network outages.

4. Blackcat is a notable cybergroup that infiltrates healthcare institutions' internal servers through vulnerabilities in their networks. The group uses "ransomware to identify and attack 'high-value victim institutions[.]'"[1] According to the Department of Justice, Blackcat typically steals victims' data and encrypts the institution's data, networks, and servers, blocking the institution from accessing them. The group then demands the institution pay a ransom in exchange for the keys to decrypt the institution's network and servers. In exchange for ransom, Blackcat also offers a promise that it will not publish the institution's data to Blackcat's site on the Dark Web. Still, even when ransoms are paid, this data often ends up on the Dark Web. Blackcat has emerged as the second most prolific ransomware-as-a-service variant in the world.[2]

5. Change stored highly sensitive information for millions of people, including active-duty US military personnel, on its servers. Such information included Personal Identifiable Information (phone numbers, addresses, Social Security numbers, etc.) ("PII") and Personal Health Information (medical, dental, and insurance records, claims information, etc.) ("PHI").[3] Blackcat accessed, copied, and exfiltrated massive amounts of this information.

---

[1] James Farrell, *Change Healthcare Blames 'Blackcat' Group for Cyber Attack That Disrupted Pharmacies and Health Systems*, FORBES (Feb. 29, 2024, 1:18 PM), https://www.forbes.com/sites/jamesfarrell/2024/02/29/change-healthcare-blames-blackcat-group-for-cyber-attack-that-disrupted-pharmacies-and-health-systems/?sh=589769fc1c4d.

[2] *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant*, DOJ (Dec. 19, 2023), https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.

[3] *MMRG Notifies Patients of Cybersecurity Incident*, BUSINESS WIRE (Feb. 6, 2024, 5:30 PM), https://www.businesswire.com/news/home/20240206060527/en/.

6. As a subsidiary of one of the largest healthcare insurers, Change processes 15 billion transactions annually, "touching one in three U.S. patient records."[4] This Data Breach has wreaked havoc on the healthcare industry, and the repercussions will continue. To blunt the effects of the Data Breach, Change took certain systems offline. One of these systems is the Change Healthcare platform ("Change Platform"). This platform provides, among other things, a revenue and payment cycle management service that connects payers, providers, and patients within the U.S. healthcare system.[5] The Change Platform is widely used among practitioners.

7. Disruption of the Change Platform has paralyzed the healthcare industry, with patients being unable to get their vital medications. Patients with chronic illnesses will suffer life-threatening symptoms without their medications. This is also a dire situation for elderly patients who cannot afford medications without insurance. Change's network outage is jeopardizing the health of millions of Americans.

8. Victims of the Data Breach include more than patients. The damage extends to healthcare providers' practices, whose claims are processed through Change, as well as hospitals. According to John Riggi, national advisor for cybersecurity and risk at the American Hospital Association, "… [T]his cyberattack has affected every hospital in the country one way or another."[6] Many providers are having trouble verifying patient eligibility and coverage, filing

[4] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access: "These are threats to life,"* CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/.
[5] *Revenue Cycle Management*, CHANGE HEALTHCARE, https://www.changehealthcare.com/revenue-cycle-management (last visited Mar. 7, 2024).
[6] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access: "These are threats to life,"* CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/.

claims, and billing patients.[7] For weeks, these healthcare practices have received little, if any, reimbursement from insurers for patient visits. Without normal cash flow from these reimbursements, small and mid-sized practices may be unable to sustain operations, as they cannot afford employee payroll, rent/mortgage, and medical supplies.

9. Exacerbating this crisis, Change has not provided adequate guidance to healthcare providers. Healthcare providers must notify their patients that their PHI may have been compromised by the Data Breach. And, under certain conditions, they must report this breach to the federal government. However, Change has not provided adequate accounts about the Data Breach that would allow healthcare providers to satisfy their obligations. Without Change's guidance, healthcare providers are in a state of uncertainty.

10. As a result of Change's negligence, healthcare providers will feel the impact of the Data Breach and network outage for some time. As the outage stretched into weeks, many healthcare providers faced the prospect of going out of business. To avert disaster, healthcare providers are incurring extra costs from switching to different claim processing platforms to assist with revenue and payment management. Small and mid-sized practices are harmed the most, as they continue to treat patients, adjust to a new system, and pay for another service, all while they are weeks behind on receiving payment.

11. Despite the disruption in its services and its failure to connect with healthcare providers, Change still manages to collect payment from subscribers.

12. Change failed to implement reasonable security measures and failed to disclose material facts regarding its deficient security protocols. Change claims that it took systems offline

[7] Associated Press, *Minnetonka Based United Healthcare Hacked*, KNSI (Feb. 29, 2024, 5:46 PM), https://knsiradio.com/2024/02/29/minnetonka-based-united-healthcare-hacked/.

to prevent the hackers from taking more data. However, this decision affected patients, as well as healthcare providers who rely on the Change Platform for processing claims and payment. Plaintiff and Class members have not received payments for their healthcare services and have incurred extra costs from switching to another healthcare payment software.

13. "An urgent care chain in Ohio may be forced to stop paying rent and other bills to cover salaries. In Florida, a cancer center is racing to find money for chemotherapy drugs to avoid delaying critical treatments for its patients. And in Pennsylvania, a primary care doctor is slashing expenses and pooling all of her cash — including her personal bank stash — in the hopes of staying afloat for the next two months."[8] This is reality for many healthcare providers as a result of Change's response following what might be the most consequential data breach in history.

14. As a direct and proximate result of Defendant's failures, Plaintiff and the Class Members have suffered serious injury.

15. Accordingly, Plaintiff, on behalf of himself and similarly situated healthcare providers who were harmed by the Data Breach and ransomware attack, seeks to hold Defendant responsible for harms caused by Defendant's failure to act.

PARTIES

16. Plaintiff Jeffrey Sklar, DC is a Pennsylvania healthcare provider with his office in Philadelphia, Pennsylvania.

17. Defendant Change Healthcare Inc. is a Delaware corporation with its principal place of business in Nashville, Tennessee.

[8] Reed Abelson & Julie Creswell, *Cyberattack Paralyzes the Largest U.S. Healthcare Payment System*, NYTIMES (Mar. 7, 2024), https://www.nytimes.com/2024/03/05/health/cyberattack-healthcare-cash.html.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members and at least some members of the proposed Class have a different citizenship from Change. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

19. This Court has jurisdiction over Change because it maintains and operates its headquarters in this District and/or is authorized to and does conduct business in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b)(1) & (2) because Change resides in this District and/or a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

Change's Privacy Practices

21. Change Healthcare is a healthcare technology company that provides data-driven and analytics-driven solutions for clinical, financial, administrative, and patient management to healthcare providers.[9] It holds itself out as providing "data and analytics, plus patient engagement and collaboration tools" to "providers and payers [to] optimize workflows, access the right information at the right time, and support the safest and most clinically appropriate care."[10] Change is one of the largest processors of prescription medications in the United States and handles billing

[9] *OptumInsight and Change Healthcare Combine to Advance a More Modern, Information and Technology-Enabled Health Care Platform*, OPTUM (Jan. 6, 2021), https://www.optum.com/en/about-us/news/page.hub.optuminsight-change-healthcare-combine.html.

[10] *The Change Healthcare Platform*, CHANGE HEALTHCARE, https://www.changehealthcare.com/platform (last visited Mar. 1, 2024).

for more than 67,000 pharmacies across the country through which it handles 15 billion healthcare transactions annually.[11]

22. As part of its business practices, Change collects and stores patients' highly sensitive PHI from healthcare providers, Medicare, and pharmacies. This includes names, addresses, Social Security numbers, medical records, insurance information, and much more.

23. Given the amount and sensitive nature of the data it stores, Change maintains a privacy policy describing how confidential and personal information is used and disclosed: "[w]e implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse. These measures are aimed at providing on-going integrity and confidentiality of data, including your personal information."

24. Change's history of handling highly sensitive PHI and its representations regarding data security show that it understood its duty to protect patients' PHI.

The Data Breach

25. On February 21, 2024, in an SEC filing, UHG announced that "a suspected nation-state associated cyber security threat actor had gained access to some of the Change Healthcare information technology systems."[12] After detecting the breach, UHG claimed to have "proactively isolated the impacted systems from other connecting systems…"[13] UHG also said it was "working with law enforcement" and allegedly "notified customers, clients and certain government

[11] Zack Whittaker, *UnitedHealth confirms ransomware gang behind Change Healthcare hack amid ongoing pharmacy outages*, TECHCRUNCH (Feb. 29, 2024, 9:15 AM) https://techcrunch.com/2024/02/29/unitedhealth-change-healthcare-ransomware-alphv-blackcat-pharmacy-outages/.
[12] *UnitedHealth Group Incorporation Form 8-K*, SEC (Feb. 21, 2024), https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm.
[13] Id.

agencies" of the breach.[14] UHG disclosed that the "network interruption [was] specific to Change Healthcare…"[15]

26. Blackcat disclosed that the exfiltrated data includes millions of: "active US military/navy personnel PII," "medical records," "dental records," "payments information," "Claims information," "Patients PII including Phone numbers/addresses/SSN/emails/etc…," "3000+ source code files for Change Health solutions…," "Insurance records," and "many many more." Blackcat warned UHG that "you are walking on a very thin line be careful you just might fall over."

27. Following the Data Breach, Change disconnected its platform. Healthcare providers—who have paid for this service—submit insurance claims through the platform. Change sends the claims to health insurance companies for evaluation and processing. Providers then receive reimbursement payments from the insurance company.

28. The Change Platform was inoperable from the time of the breach and was projected to remain inoperable through at least mid-March.[16] On March 18, 2024, Change notified customers that it was back up and that reconnection for most customers was expected by the week of March 25, 2024.

29. Given that the Change Platform handles 15 billion healthcare transactions (or about one-in-three U.S. patient records), its outage disrupted a massive amount of healthcare providers' claims. Moreover, for the many providers whose claims are *only* processed through Change, their payments were completely stopped.

---

[14] Id.
[15] Id.
[16] https://www.unitedhealthgroup.com/changehealthcarecyberresponse (last visited March 13, 2024)

30. The potential impact of the Data Breach is enormous, and its effects are currently being felt by healthcare providers nationwide.

The Data Breach Was Preventable

31. Change's cybersecurity practices and policies were inadequate and fell short of the industry-standard measures that should have been implemented long before the Data Breach occurred. This is especially true given that the healthcare industry is frequently one of the most targeted sectors for cyberattacks. Attacks using stolen credentials have increased precipitously over the last several years.

32. A ransomware attack adds an extra layer of seriousness over a data breach. Whereas a standard breach involves the exfiltration and criminal use of personal information, a ransomware attack locks the network and makes it completely inaccessible to the enterprise or computer user. In the case of healthcare services, the consequences can be life or death.

33. Due to the highly sensitive PHI that is maintained in the healthcare system, providers and their affiliates like Change are prime targets of cyberattacks. Even if no sensitive or health information is disseminated, the risks to patient treatment, health, and safety are significantly increased because of the serious and even life-threatening consequences presented by even a short-lived interruption of healthcare services.

34. This was known and obvious to Change as it observed frequent public announcements of data breaches affecting healthcare providers and knew that information of the type it collected, maintained, and stored is highly coveted and a frequent target of hackers and ransomware attacks. For example, in early 2016, the Hollywood Presbyterial Medical Center in

Los Angeles was the victim of a ransomware attack and opted to pay $17,000 in Bitcoin to retrieve the key to unlock its data.[17]

35. The most popular and effective method of gaining authorized access to a company's internal networks has long been the use of stolen credentials, and companies should activate defenses to prevent such attacks.

36. According to the Federal Bureau of Investigation (FBI), phishing schemes designed to induce individuals to reveal personal information, such as network passwords, were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[18] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[19]

37. The risk is so prevalent for healthcare providers that on October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[20] The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (HHS), and the FBI issued the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[21]

---

[17] Richard Winton, Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating, The LA Times (Feb. 18, 2016), http://www.latimes.com/business/technology/la-me-In-hollywood-hospital-bitcoin-20160217-story.html (last visited April 1, 2024)

[18] *2020 Internet Crime Report*, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Mar. 1, 2024).

[19] *2021 DBIR Master's Guide*, VERIZON, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited Mar. 1, 2024).

[20] *Ransomware Activity Targeting the Healthcare and Public Health Sector*, JOINT CYBERSECURITY ADVISORY, https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited Mar. 1, 2024).

[21] *Id*.

38. The two main ways to lessen the risk of stolen credentials are user education and technical security barriers.

39. User education involves teaching network users about common disclosure schemes and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients.

40. Technical security barriers include software that scans all incoming messages for harmful attachments or malicious content and certain security measures governing e-mail transmissions, including Sender Policy Framework (SPF) (e-mail authentication method used to prevent spammers from sending messages on behalf of a company's domain), DomainKeys Identified Mail (DKIM) (e-mail authentication method used to ensure messages are not altered in transit between the sending and recipient servers), and Domain-based Message Authentication, Reporting and Conformance (DMARC), which "builds on the widely deployed [SPF] and [DKIM] protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email."[22]

41. In addition to mitigating the risk of stolen credentials, the CISA guidance encourages organizations to prevent unauthorized access by:

- Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;
- Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;
- Ensuring devices are properly configured and that security features are enabled;

[22] *Id*.

- Employing best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and
- Disabling operating system network file sharing protocol known as Server Message Block (SMB) which is used by threat actors to travel through a network to spread malware or access sensitive data.[23]

42. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[24] Likewise, the principle of least privilege (POLP) to all systems should be applied to all systems so that users only have the access they need to perform their jobs.[25]

43. Despite its vital role in the healthcare industry, Change failed to follow the CISA recommended best practices. Indeed, had Change implemented common sense security measures like network segmentation and POLP, the hackers never could have accessed millions of patient files and the breach would have been prevented or much smaller in scope. Further, Change lacked essential and available safeguards to prevent and detect phishing attacks and failed to implement adequate monitoring or control systems to detect the unauthorized infiltration after it occurred.

44. Change should have known that it was an attractive target for cybercriminals and should have implemented robust protections for the vast amounts of sensitive data that it stored. Cybersecurity measures could have detected and terminated a breach before it could expand in

[23] CISA Guide at 4.
[24] *Id.* at 5.
[25] *Id*. at 6.

scope and impact. Change's failure to comply with industry standards is unreasonable given its knowledge that it was a prime target for cyberattacks.

The Aftermath of the Data Breach

45. As a result of the Data Breach, Change shut down most of its network including its Change Platform used by healthcare providers nationwide in connection with payment and treatment. Change took this action without an adequate alternative, and this choice is decimating healthcare practices nationwide.

46. Because Change disconnected the Change Platform, many healthcare providers have lost their primary (and in some cases their *only*) source of processing payments for their services through patients' healthcare plans and thus are not receiving payment. Healthcare providers are absorbing these upfront costs.

47. A dwindling account balance coupled with outstanding reimbursement has put many healthcare providers in a precarious position. For instance, Arlington Urgent Care, a chain of five urgent care centers around Columbus, Ohio, has about $650,000 in unpaid insurance reimbursements. The owners have taken lines of credit from banks and used their personal saving to afford employee payroll, rent, and other expenses.[26] Other healthcare providers are racking up duplicated payment software charges. Florida Cancer Specialists and Research Institute in Gainesville switched to two other healthcare software platforms because "it spends $300 million a month on chemotherapy and other drugs for patients whose treatments cannot be delayed."[27] And some healthcare providers are cutting resources for patients to persevere through this. A

[26] Reed Abelson & Julie Creswell, *Cyberattack Paralyzes the Largest U.S. Healthcare Payment System*, NYTIMES (Mar. 7, 2024), https://www.nytimes.com/2024/03/05/health/cyberattack-healthcare-cash.html.
[27] *Id*.

Philadelphia-based primary care practice with 20 clinicians has mailed off "hundreds and hundreds" of pages Medicare claims and is contemplating cutting expenses by "reducing the supply of vaccines the clinic has on hand."[28]

48. Healthcare providers paid for Change's services that they are not receiving, and without these services, providers and practices are struggling to care for patients and are losing money.

Allegations Relating to Plaintiff Jeffrey Sklar, DC

49. Jeffrey Sklar, DC is a Pennsylvania healthcare provider with his office located at 15 W. Highland Ave, Philadelphia, Pennsylvania.

50. Dr. Jeffrey Sklar maintains a specialized chiropractic center in Philadelphia. He has practiced chiropractic medicine for over 24 years.

51. Like most medical practices, especially sole proprietorships, Dr. Sklar depends on timely processing of insurance claims to operate and fund his practice. A bulk of his charges foe medical services provided to his patients are paid through insurance. The funds Dr. Sklar receives through insurance payments are necessary to operate his practice and treat patients. Those funds are crucial, for example, to Dr. Sklar paying bills, for supplies and equipment, rent, insurance, other expenses and costs. In addition, as the sole proprietor those funds are critical as it is Dr. Sklar's source of revenue.

52. On or around May 10, 2022, Plaintiff contracted with Medical Billing Professionals to process his patient's insurance claims and to get timely paid on those claims.

53. Medical Billing Professionals used the Change Platform to submit bills/reimbursement forms to insurers on behalf of its clients like Dr. Sklar.

[28] *Id*.

54. On or around February 22, 2024, Plaintiff learned that his processing of payment of medical bills had been affected as a result of the Data Breach. Though Change has not communicated directly with Dr. Sklar, he has been informed that the disruption of processing and payment of his bills is the result of Change's decision to disconnect the network after the Data Breach.

55. This disconnection was reasonably foreseeable to Change due to the failure to protect its network from cyberattacks.

56. Once the Data Breach occurred and Change disabled the Change Platform, Dr. Sklar was unable to submit reimbursement requests/bills on behalf of his patients which completely disrupted his practice and his livelihood.

57. Dr. Sklar continued to treat patients during the Change outage, without any certainty about when payment would be received.

58. Over the ensuing weeks since Change disabled the Change platform, the ordinary and timely processing of insurance claims for Dr. Sklar's services has continued to be stalled and completely disrupted which has had a devasting effect on his practice and Dr. Sklar. The cash flow that Dr. Sklar normally would receive through insurance payments was nonexistent. As of March 26, 2024, Dr. Sklar had $29,505 of outstanding medical bills that were not processed due to the Change outage, forcing Dr. Sklar to divert funds to operate and fund his practice. The disruption of and threat to his beloved practice, along with the increased financial pressure, has caused Dr. Sklar substantial financial and emotional distress.

59. Upon the recommendation of Medical Billing Professionals, Dr. Sklar enrolled with another platform for submitting bills. As a result, Dr. Sklar incurred additional setup and

processing costs for his reimbursement requests. In addition, this switch was also significantly time-consuming requiring Dr. Sklar to divert his time and energy to dealing with this crisis.

60. More recently, Medical Billing Professionals switched to a different platform, the second change in two weeks, causing even more of a disruption to Dr. Sklar's practice.

61. Enrollment in this new platform adds a considerable monthly cost to the fees that Dr. Sklar pays for billing services. Further, Dr. Sklar is spending an exorbitant amount of time completing applications and learning yet another platform, requiring Dr. Sklar to divert his time and energy to dealing with this crisis.

62. This billing nightmare has forced Dr. Sklar to spend significant time away from patient treatment, which has affected the operation of his practice and his ability to treat and care for his patients.

63. Due to the inability to submit bills and get paid for services rendered to his patients after the Change Platform was disabled, Dr. Sklar experienced a backlog of unpaid revenues, which as described above has impacted his ability to operate and run his practice including paying bills, for supplies and equipment, rent, insurance, other expenses and costs. In addition, as the sole proprietor Dr. Sklar's revenue has substantially been decreased.

Change Failed to Comply with Federal Law and Regulatory Guidance

64. Change is covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (see 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

65. These rules establish national standards for the protection of patient information, including PHI, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

66. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[29]

67. HIPAA requires that Change implement appropriate safeguards for this information.[30]

68. HIPAA requires that Change provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—i.e. non-encrypted data.[31]

69. Despite these requirements, Change failed to comply with its duties under HIPAA and its own privacy policies. Indeed, Change failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Adequately protect the PHI of patients;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to

[29] 45 C.F.R. § 164.502.
[30] 45 C.F.R. § 164.530(c)(1).
[31] 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

70. Further, businesses holding sensitive data have been provided with authoritative and publicly available resources to help reduce the risks of cyberattacks. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance

of reasonable data security practices, which should be factored into all business-related decision making.[32]

71. The FTC's publication *Protecting Personal Information: A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[33] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[34]

72. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[35] This is consistent with guidance provided by the FBI, HHS, and the principles set forth in the CISA 2020 guidance.

73. Businesses that fail to reasonably protect customer information have been subjected to FTC enforcement actions. The FTC treats failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or

---

[32] *Start with Security*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Mar. 1, 2024).
[33] *Protecting Personal Information*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 1, 2024).
[34] *Id*.
[35] *Start With Security*, supra note 32.

practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[36]

74. Despite being fully aware of its duty to safeguard patients' PHI, Change failed to follow basic recommendations and guidelines that would have prevented this breach from occurring. Further, Change failed to take action despite knowledge of other cyberattacks. Change's failure to employ reasonable cybersecurity measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

75. Plaintiff seeks relief in his individual capacity and as a representative of all others who are similarly situated. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff brings this action on behalf of himself and the Class defined as:

> All healthcare providers whose reimbursement payments were delayed following the Data Breach announced by UnitedHealth Group Incorporated in February 2024.

76. Specifically excluded from the Class are Defendant; its officers, directors, or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant.

77. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

[36] *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Mar. 1, 2024).

78. Class Identity: The members of the Class are readily identifiable and ascertainable. Change and/or its affiliates, among others, possess the information to identify and contact class members.

79. Numerosity: The members of the Class are so numerous that joinder of all of them is impracticable. According to the U.S. Department of Health and Human Services, Change "processes 15 billion health care transactions annually and is involved in one in every three patient records." According to Change, it is connected to "more than 600,000 providers[.]"

80. Typicality: Plaintiff's claims are typical of the claims of the members of the Class because all class members reimbursement payments were delayed following the Data Breach and were harmed as a result.

81. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has no known interest antagonistic to those of the Class and its interests are aligned with Class members' interests. Plaintiff's reimbursement payments were delayed following the Data Breach just as class members and suffered similar harms. Plaintiff has also retained competent counsel with significant experience litigating complex and commercial class actions.

82. Commonality and Predominance: There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual class members. The common questions of law and fact include, without limitation:

- Whether Change owed Plaintiff and class members a duty to implement and maintain reasonable security procedures and practices to protect patients' PHI;
- Whether Change acted negligently in connection with the monitoring and/or protection of Plaintiff's and class members' PHI;

- Whether Change violated its duty to implement reasonable security systems to protect Plaintiff's and class members' PHI;
- Whether Change's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and class members;
- Whether Change adequately addressed and fixed the vulnerabilities that enabled the Data Breach;
- Whether class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

83. Change has engaged in a common course of conduct and Plaintiff and class members have been similarly impacted by Change's failure to maintain reasonable security procedures and practices to protect patients' PHI.

84. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

85. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

86. Change required patients' PHI as a condition of receiving healthcare services and to perform Change's functions in connection with patients receiving medical treatment. Change stored the data for purposes of providing health insurance services as well as for commercial gain.

87. Change owed Plaintiff and class members a duty to exercise reasonable care in protecting patients' PHI from unauthorized disclosure or access. Change acknowledged this duty in its privacy policies, where it promised not to disclose PHI, including SSNs, without authorization and to abide by all federal laws and regulations.

88. Change owed a duty of care to Plaintiff and class members to provide adequate data security, consistent with industry standards, to ensure that Change's systems and networks adequately protected the PHI.

89. Defendant's duty to use reasonable care in protecting PHI arises from common law and federal law, including the HIPAA regulations described above and Change's own policies and promises regarding privacy and data security.

90. Change knew, or should have known, of the risks inherent in collecting and storing PHI in a centralized location, Change's vulnerability to network attacks, and the importance of adequate security.

91. Plaintiff and class members were foreseeable and probable victims of any inadequate cybersecurity practices.

92. Change breached its duty to Plaintiff and class members in numerous ways, as described herein, including by:

- Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect patients' PHI;
- Failing to comply with industry standard data security measures for the healthcare industry leading up to the Data Breach;
- Failing to comply with its own privacy policies;
- Failing to comply with regulations protecting the PHI at issue during the period of the Data Breach; and
- Failing to adequately monitor, evaluate, and ensure the security of Change's network and systems;

93. Patients' PHI would not have been compromised but for Change's wrongful and negligent breach of its duties.

94. Change would not have disconnected the Change Platform but for its wrongful and negligent breach of its duties.

95. Given that healthcare providers and affiliates are prime targets for hackers, Change's failure to take proper security measures to protect patients' PHI, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and copying of PHI by unauthorized third parties. It was also foreseeable that as a result of a data breach, Change would have to disconnect systems that could disrupt healthcare practices.

96. As a direct and proximate result of Change's conduct, Plaintiff and class members have suffered damages, including missed payments and out-of-pocket expenses associated with (i) purchasing new healthcare payment software; (ii) notifying patients of data breach; and (iii) late penalties assessed for untimely payment of expenses. Furthermore, Plaintiff and class members'

damages include time and effort spent researching and implementing new healthcare payment software.

COUNT TWO
NEGLIGENT UNDERTAKING
(On Behalf of Plaintiff and the Class)

97. Plaintiff restates and re-alleges every allegation of the preceding paragraphs of this Complaint.

98. By agreeing to serve as a claims clearinghouse and payment processor, Defendant undertook to render revenue and claims processing services that benefited Plaintiff and class members.

99. In undertaking to provide such services, Defendant knew or should have known of the necessity to heed credible security warnings, maintain adequate cybersecurity policies and procedures, detect alerts in regard to vulnerabilities affecting its systems, and implement appropriate procedures to keep security current and address vulnerabilities.

100. Only Defendant was in the position to ensure that its information systems, practices, and protocols were sufficient and consistent with industry standards and requirements.

101. Defendant failed to exercise reasonable care to perform these actions. Defendant failed to engage in appropriate cybersecurity practices to safeguard their claims processing and revenue cycle services on behalf of Plaintiff and class members.

102. Defendant's failure to abide by its duties placed Plaintiff and class members in a worse position than they would have been had Defendant not undertaken such duties because other, more secure means would have been used to process insurance claims and payments for Plaintiff's practice and those of the Class which would have avoided the current disruption and lack of funds flowing to Plaintiff and the Class.

103. Defendant's failure to abide by its duties was wrongful and negligent in light of the foreseeable risks and known threats.

104. Defendant knew or should have known that failure to take appropriate actions to secure its systems increased the risk of harm to Plaintiff and class members beyond the risk of harm that existed without the undertaking.

105. As a direct and proximate result of Defendant's negligent undertaking, Plaintiff and the class members have suffered and will suffer injury.

COUNT THREE
NEGLIGENT FAILURE TO WARN
(On Behalf of Plaintiff and the Class)

106. Plaintiff restates and re-alleges every allegation of the preceding paragraphs of this Complaint.

107. Upon information and belief, Defendant had been aware for a substantial period of time that its cybersecurity systems and networks were inadequate and prone to attack.

108. Defendant knew or should have known of its cybersecurity failures including, but not limited to, failing to heed credible security warnings; failing to maintain adequate patch management policies and procedures; failing to detect alerts in regard to vulnerabilities affecting its systems; failing to properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat; failing to properly use automated tools to track which versions of software were running and whether updates were available; and failing to implement appropriate procedures to keep security current and address vulnerabilities, including to monitor expert websites and software vendors' websites regularly for alerts about new vulnerabilities.

109. Nevertheless, Defendant failed to warn Plaintiff and Class Members of the known cybersecurity vulnerabilities, failed to effectively remedy the cybersecurity flaws and problems in their systems and networks, failed to warn Plaintiff and Class Members of likely risks caused by Defendant's failure to remedy such cybersecurity flaws, and failed to provide prompt notice to Plaintiff and Class Members that the promised secure information systems had been breached by unauthorized persons during the Cyberattack.

110. As a direct and proximate result of Defendant's negligent failure to warn, Plaintiff and the class members have suffered and will suffer injury.

COUNT IV
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

111. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

112. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

113. An actual controversy has arisen in the wake of the Data Breach regarding Change's present and prospective common law and other duties to reasonably safeguard PHI and whether Change is currently maintaining data security measures adequate to protect patients from further cyberattacks and data breaches that could compromise their PHI and therefore prevent healthcare providers from remaining without use of the Change Platform, which is a lynchpin of their payment practices.

114. Change still possesses PHI pertaining to Plaintiff and class members, which means the PHI remains at risk of further breaches because Change's data security measures remain

inadequate. Another data breach would likely result in Change disconnecting the Change Platform again causing further injuries to Plaintiff and class members.

115. Pursuant to the Declaratory Judgment Act, Plaintiff seeks a declaration that: (a) Change's existing data security measures do not comply with its obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) Change must have policies and procedures in place to ensure the parties with whom it shares sensitive personal information maintain reasonable, industry-standard security measures, including, but not limited to, those listed at (ii), (a)-(i), infra, and must comply with those policies and procedures; (2) Change must: (i) purge, delete, or destroy in a reasonably secure manner patients' PHI if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Change's systems on a periodic basis, and ordering Change to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Encrypting PHI and segmenting PHI by, among other things, creating firewalls and access controls so that if one area of Change's systems is compromised, hackers cannot gain access to other portions of its systems;

e. Purging, deleting, and destroying in a reasonable and secure manner PHI not necessary to perform essential business functions;

f. Conducting regular database scanning and security checks;

g. Conducting regular employee education regarding best security practices;

h. Implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and

i. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class set forth herein, respectfully requests the following relief:

a. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representatives and Plaintiff's counsel as Class Counsel;

b. That the Court grant permanent injunctive relief to prohibit and prevent Change from continuing to engage in the unlawful acts, omissions, and practices described herein;

c. That the Court award Plaintiff and class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

d. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

e. That Plaintiff be granted the declaratory and injunctive relief sought herein;

f. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

g. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial in the instant action.

Dated: April 4, 2024

Respectfully submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV, BPR 23045
Grayson Wells BPR #039658
Michael Iadevaia, BPR 041622
Emily Schiller, BPR 039387
STRANCH, JENNINGS & GARVEY PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com
miadevaia@stranchlaw.com
eschiller@stranchlaw.com

LEVIN SEDRAN & BERMAN LLP
Charles E. Schaffer *
510 Walnut St., Ste 500
Philadelphia, PA 19106
Tel: (215) 592-1500
cschaffer@lfsblaw.com

LEEDS BROWN LAW, P.C.
Jeffrey K. Brown *
Brett R. Cohen *
One Old Country Road, Suite 347
Carle Place, NY 11514-1851
Tel: (516) 873-9550
jbrown@leedsbrownlaw.com
bcohen@leedsbrownlaw.com

GOLDENBERG SCHNEIDER, LPA
Jeffrey S. Goldenberg *
Todd B. Naylor *
4445 Lake Forest Dr., Ste. 490
Cincinnati, OH 45242
Tel: (513) 345-8291
jgoldenberg@gs-legal.com
tnaylor@gs-legal.com

Counsel for Plaintiff & the Putative Class

*Pro hac vice forthcoming **